PALM BEACH STATE COLLEGE

Research Assignment #4 Instructions

Subject: SSL & TLS

Your paper should include, but is not limited to:

What is SSL & TLS used for? Technically and practically.
How does SSL/TLS help secure the internet?
What technologies and techniques have we studied that have been incorporated into SSL/TLS?
Why have these technologies and techniques been incorporated into SSL/TLS?
How do you know if a site is using SSL?

Discuss how SSL & TLS work.
Make sure to discuss ALL the steps in the handshake.
Explain why hashing is important to this protocol.
Include at least a brief explanation of the concept of public/private key and; how it works.
Explain how the public/private key protocol is used in SSL.
Discuss the weaknesses in previous levels that led to the evolution of SSL to TLS and the different release levels.

Extra points for explaining the math involved in public/private key protocols.

Remember:

You are graded on grammar, spelling and punctation as well as your content.
There is a 1/2 point deduction for each error that your paper generates on www.languagetool.org
There is a 1/2 point deduction for not defining a term before using it.
There is a 1/2 point deduction for not defining an abbrevation properly.
Ex. All Abbreviations Must Be Defined (AAMBD)
There is a 1/2 point deduction for not defining an abbrevation before using it.
Wikipedia is not a citation. There is a 10 point deduction for citing Wikipedia.